UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Seizure of Up to $217,166.77 of monies, funds, monetary instruments, stocks, bonds, cryptocurrencies (including, but not limited to, Bitcoin and Tether), securities, private keys, recovery seeds, and any other property in, credited to, or associated with the Binance account of user id 127986473 held in the user name Richard Adeyemi Oluwafemi	)	Case No. 4:23MJ7353 SPM

APPLICATION AND AFFIDAVIT FOR SEIZURE WARRANT

I, Eric Field, being duly sworn depose and say:

I am a Special Agent with the Federal Bureau of Investigation, and have reason to believe that there is now certain property namely

Up to $217,166.77 of monies, funds, monetary instruments, stocks, bonds, cryptocurrencies (including, but not limited to, Bitcoin and Tether), securities, private keys, recovery seeds, and any other property in, credited to, or associated with the Binance account of user id 127986473 held in the user name Richard Adeyemi Oluwafemi

which is

subject to forfeiture under Title 18, United States Code, Sections 981(a)(1) and 982(a)(1) and Title 28, United States Code, Section 2461, and therefore, is subject to seizure under Title 18, United States Code, Sections 981(b)& 982(b) and Title 21, United States Code, Sections 853(e)&(f) concerning violations of Title 18, United States Code, Sections 1343 and 1956.

The facts to support a finding of Probable Cause for issuance of a Seizure Warrant are as follows:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

Continued on the attached sheet and made a part hereof. X **Yes** ___ **No**

Signature of Affiant, Special Agent Eric Field

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41

September 15, 2023 at 14:48
Date and Time Issued

at St. Louis, Missouri
City and State

Honorable Shirley P. Mensah, U.S. Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEIZURE WARRANT

I, Eric Field, a Special Agent with the United States Federal Bureau of Investigation ("FBI"), being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent with the FBI since June 2009. I am currently assigned to investigate cybercrimes. Before that, I was involved in investigations relating to public corruption, mortgage fraud, theft of federal funds, and other white-collar crimes. Prior to my employment as a Special Agent with the FBI, I worked as a Certified Public Accountant and Certified Fraud Examiner in the audit sector of public accounting.

2. As a Special Agent with the FBI, I have received significant training on how people use computers to commit crimes and on law enforcement techniques that can be utilized to investigate and disrupt such crimes. In the course of my investigations and other cases on which I have worked, I have gained experience executing seizure warrants, as well as search warrants for physical premises and for electronic evidence and data, including the content and other data associated with email, messenger, financial, and digital-marketplace accounts operating on both the traditional Internet and the dark web.

3. The information contained in this affidavit is based on statements and information obtained from witnesses and other law enforcement officers, my personal knowledge and observations during the course of this investigation, my personal training and experience as a criminal investigator, and my review of records, documents, and other evidence obtained during this investigation. Because this affidavit is being submitted for the limited purpose of establishing probable cause for the requested seizure warrant, I have not included in this affidavit all facts

known to me concerning this investigation. Rather, I have included in this affidavit only those facts that I believe are necessary to establish probable cause for the requested seizure warrant.

PROPERTY TO BE SEIZED

4. This affidavit is submitted in support of a seizure warrant for the following property:

> Up to $217,166.77 of monies, funds, monetary instruments, stocks, bonds, cryptocurrencies (including, but not limited to, Bitcoin and Tether), securities, private keys, recovery seeds, and any other property in, credited to, or associated with the Binance account of user id 127986473 held in the user name Richard Adeyemi Oluwafemi (the "**Subject Account**").

5. As set forth below, there is probable cause to believe that the property in the **Subject Account** is subject to seizure and forfeiture as property constituting, or derived from, proceeds obtained, directly or indirectly, as the result of violations of 18 U.S.C. § 1343 (wire fraud) and/or 18 U.S.C. § 1956 (money laundering).

LEGAL FRAMEWORK

6. The proceeds of wire fraud and/or money laundering are subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A), (C), and (D), and to criminal forfeiture pursuant to 18 U.S.C. §§ 981(a)(1), 982(a)(1) and (2)(A), and 28 U.S.C. § 2461(c). This application seeks a seizure warrant under both civil and criminal authority because the property in the **Subject Account** could be placed beyond process if not seized by warrant.

7. The civil forfeiture statute, 18 U.S.C. § 981, provides that property subject to civil forfeiture may be seized by a civil seizure warrant issued by a judicial officer "in any district in which a forfeiture action against the property may be filed under section 1355(b) of title 28," and

may be executed "in any district in which the property is found," if there is probable cause to believe that the property is subject to forfeiture. 18 U.S.C. § 981(b)(3).

8. In turn, 28 U.S.C. § 1355(b) provides, in pertinent part, that a civil forfeiture action may be filed in any district where "acts or omissions giving rise to the forfeiture occurred[.]" 28 U.S.C. § 1355(b)(1)(A).

9. Thus, notwithstanding the provisions of Rule 41(a) of the Federal Rules of Criminal Procedure, the issuance of this seizure warrant in this district is appropriate under 18 U.S.C. § 981(b)(3) and 28 U.S.C. § 1355(b)(1)(A) because, as detailed below, acts or omissions giving rise to the wire fraud and/or money laundering scheme under investigation occurred in the Eastern District of Missouri, in that the scheme involved wire transfers made to and from a Missouri bank.

10. The criminal forfeiture statute, 18 U.S.C. § 982(b)(1), incorporates the provisions of 21 U.S.C. § 853 (other than subsection (d)) for a criminal forfeiture action. Section 853(f) authorizes the issuance of a seizure warrant for property subject to criminal forfeiture. In addition, 28 U.S.C. § 2461(c) provides that, "[i]f a person is charged in a criminal case with a violation of an Act of Congress for which the civil or criminal forfeiture of property is authorized," then the United States can obtain forfeiture of property "as part of the sentence in the criminal case." Thus, pursuant to 28 U.S.C. § 2461(c) and 18 U.S.C. § 981(a)(1)(C), any property, real or personal, which constitutes, or is derived from, proceeds traceable to wire fraud, is subject to criminal forfeiture.

11. Based on the foregoing, the issuance of this seizure warrant is authorized under 18 U.S.C. §§ 981(b) for civil forfeiture, and under 21 U.S.C. § 853(f) and 18 U.S.C. § 982(b)(1) for criminal forfeiture.

BACKGROUND ON CRYPTOCURRENCY

12. Cryptocurrency is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[1] Cryptocurrency is stored in a virtual account called a "wallet." Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency.

13. Bitcoin and Tether are two types of cryptocurrencies. Payments or transfers of value made with Bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. Tether does not have its own dedicated blockchain. Instead, payments or transfers of value made with Tether are recorded on the blockchains of other cryptocurrencies, including the Bitcoin blockchain. Individuals can acquire Bitcoin and Tether through exchanges (*i.e.*, online companies that allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), cryptocurrency ATMs, or directly from other people. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers.

[1] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

14. Cryptocurrency "exchangers" and "exchanges" are individuals or companies that exchange cryptocurrency for other currencies, including U.S. dollars. Coinbase Global, Inc. ("**Coinbase**") is a cryptocurrency exchange headquartered in San Francisco, California. Binance Holdings Ltd. ("**Binance**") is a cryptocurrency exchange headquartered in the Cayman Islands that accepts records requests and legal process, including seizure warrants, from, among other law enforcement agencies, the FBI, by way of electronic submissions to BAM Trading at LERT@BINANCE.US. Both Coinbase and Binance broker several different types of cryptocurrencies, including Bitcoin and Tether.

15. Cryptocurrency is not illegal in the United States. Although cryptocurrencies such as Bitcoin and Tether have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes, including in connection with wire fraud and/or money laundering activities, and is an oft-used means of payment for illegal goods and services on hidden services websites operating on the Tor network. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within the dark web marketplaces.

PROBABLE CAUSE

A. The Scheme

16. On July 24, 2023, the FBI opened an investigation into unknown subjects when a local bank headquartered within the Eastern District of Missouri reported that it had been defrauded of approximately $1 million, as further detailed below.

17. The bank has a long-term client based in Phoenix, Arizona. At the time of the events detailed in this affidavit, the bank was actively seeking to increase its level of business with

the client. To that end, in March 2023, the bank began email correspondence with the client's VP of Finance regarding the client increasing its deposits at the bank.

18. At some point between March 2023 and June 2023, the email accounts of certain of the client's employees, including the VP of Finance and the President, were hacked. Specifically, unknown subjects made it so that any emails between the client's employees and the bank were segmented into a file that only the unknown subjects could view.

19. On or about June 12, 2023, the bank received an email that appeared to have been sent by the client's VP of Finance but was actually sent by an unknown subject using the VP of Finance's email address. In this email, the unknown subject requested that the client's President be set up as an administrator for the client's online banking account, and included the email address of the client's President as a carbon copy recipient of the email. Based on this email and subsequent email communications from the bank, the unknown subject learned that the client's VP of Finance was already an administrator for the client's online banking account, and received instructions on how to set up the client's President as an administrator for the client's online banking account.

20. On or about June 20, 2023, the bank received another email that appeared to have been sent by the client's VP of Finance but was actually sent by an unknown subject using the VP of Finance's email address. In this email, the unknown subject requested that the client be enrolled in ACH payment processing. The bank responded by email, requesting to schedule a call to understand the client's need for ACH payment processing.

21. Two days later, on or about June 22, 2023, the bank again received an email that appeared to have been sent by the client's VP of Finance but was actually sent by an unknown subject using the VP of Finance's email address. In this email, the unknown subject indicated that

the client did not anticipate frequent use of ACH payment processing and inquired about how long it would take to set up the ACH payment processing. The bank responded by email, in which it provided the ACH paperwork and informed the unknown subject that the ACH payment processing could be set up within two days of the bank receiving the completed paperwork.

22. After receiving the completed ACH paperwork, on or about June 27, 2023, the bank emailed the client's VP of Finance, confirming that the ACH payment processing had been set up and would be available for use the next day. Because the email of the client's VP of Finance had been hacked, the email from the bank went directly to the unknown subject and not to the client's VP of Finance.

23. On or about July 5, 2023, a credit batch in the amount of $201,368.06, with an effective date of July 6, 2023, was originated by an unknown subject from the client's bank account. The funds taken through this credit batch were in the client's bank account legitimately.

24. On or about July 6, 2023, the unknown subject, impersonating the client's VP of Finance, called the bank and requested a one-day increase of the ACH limit for the client's bank account, from $250,000 to $950,000, to accommodate a large transfer. The bank approved the increase, effective for July 7, 2023 only.

25. On or about July 7, 2023, a debit batch in the amount of $900,000, with an effective date of July 10, 2023, was originated by an unknown subject for the client's bank account. The funds that were deposited into the client's bank account via this debit batch originated from a bank account at a different bank that belonged to a New York City law firm, which had not authorized the transaction. Contemporaneous with the debit batch, a credit batch in the amount of $45,000, with an effective date of July 10, 2023, was originated by an unknown subject from the client's bank account.

26. On or about July 10, 2023, the unknown subject, impersonating the client's VP of Finance, called the bank's customer service number and requested another one-day increase of the ACH limit for the client's bank account, again from $250,000 to $950,000. The bank attempted to verify the request by calling the phone number listed in the prior emails that the bank believed had been sent by the client's VP of Finance. The call went unanswered, so the bank left a voicemail. Unbeknownst to the bank, the phone number listed in the prior emails had been altered by the unknown subject and, thus, the call and voicemail were directed to the unknown subject and not to the client's VP of Finance.

27. Later that same day, the bank received an email that appeared to have been sent by the client's VP of Finance but was actually sent by an unknown subject using the VP of Finance's email address. In this email, the unknown subject indicated that he received the voicemail but was unavailable to talk on the phone.

28. Later that same day, the unknown subject, impersonating the client's VP of Finance, called the bank's customer service number and requested another increase of the ACH limit for the client's bank account, this time to $1.9 million. The bank approved the increase, effective for July 11, 2023 only.

29. On or about July 11, 2023, a debit batch in the amount of $1,000,000, with an effective date of July 11, 2023, was originated by an unknown subject for the client's bank account. Like the July 7, 2023 debit batch, the funds that were deposited into the client's bank account through this debit batch originated from a bank account at a different bank that belonged to the New York City law firm, which had not authorized the transaction. Contemporaneous with this debit batch, three credit batches totaling $942,089.72—one for $342,450, one for $227,657.55,

and one for $371,982.17—each with an effective date of July 11, 2023, were originated by an unknown subject from the client's bank account.

30. That same day, the unknown subject, impersonating the client's VP of Finance, called the bank's customer service number and requested yet another increase of the ACH limit for the client's bank account. After the bank indicated that it would not approve the increase without a phone call, the unknown subject, impersonating the client's VP of Finance, called a bank representative. The bank representative did not believe that the person he spoke with was, in fact, the client's VP of Finance. As a result, the bank representative called the client's office and spoke with the VP of Finance, who confirmed that he had not been the person making the transactions described above.

31. After speaking with the client's VP of Finance, the bank returned to the New York City law firm all funds that the bank had received via debit batches from the law firm's bank account. The bank also attempted to reverse each of the credit batches from the client's bank account but was unsuccessful. Ultimately, the bank recovered only $472,652.58 of the $1,188,457.78 in credit batches that were originated by an unknown subject from the client's bank account. As a result, the bank suffered a loss of $715,805.20.

B. Subsequent Investigation Tracing the Scheme's Proceeds

32. Through subsequent investigation, the FBI learned that approximately $420,325 of the credit batches were sent to twelve different accounts held at Pathward, N.A. ("**Pathward**"). The FBI then served a Grand Jury subpoena on Pathward. Pathward's response to the Grand Jury subpoena disclosed that these funds were transferred to twelve accounts held at Coinbase.

33. Based on the information learned from Pathward's response, the FBI served a Grand Jury subpoena on Coinbase. After receiving the materials produced by Coinbase in

response to the Grand Jury subpoena, the FBI analyzed them and, in doing so, followed Bitcoin and other cryptocurrencies through the Blockchain. This analysis revealed that a majority of the funds from the credit batches that were transferred to the Coinbase accounts were subsequently transferred to various cryptocurrency wallets held at Binance. Specifically, the FBI's analysis uncovered that, of the approximately $420,325 in funds that were transferred from Pathward to Coinbase, approximately 8.130968 Bitcoin (with an approximate value of $217,166.77 USD as of September 14, 2023) were later transferred to a Binance wallet.

34. Based on a law enforcement request, on or about August 26, 2023, Binance provided the following information regarding the owner of the above-referenced Binance wallet: Richard Adeyemi Oluwafemi, email address richardadeyemi29@gmail.com, User ID 127986473 (*i.e.*, the **Subject Account)**. At that time, the **Subject Account** held multiple wallets with multiple different cryptocurrencies, including approximately $825,864.61 of Tether, which was equivalent to 31.77623294 of Bitcoin as of August 26, 2023.

35. Based on all of the foregoing, as well as my training, education, and experience, there is probable cause to believe that the **Subject Account** was used to launder at least as much as $217,166.77 of the proceeds of the wire fraud scheme described above.

CONCLUSION

36. Based on the foregoing, I believe that there is probable cause to seize up to $217,166.77 of monies, funds, monetary instruments, stocks, bonds, cryptocurrencies (including, but not limited to, Bitcoin and Tether), securities, private keys, recovery seeds, and any other property in, credited to, or associated with the **Subject Account** because such property constitutes proceeds of wire fraud and/or constitutes property involved in money laundering and/or is

otherwise traceable thereto, such that the property is subject to civil and criminal forfeiture pursuant to 18 U.S.C. § 981(a)(1), 18 U.S.C. § 982(a)(1) and (a)(2), and 28 U.S.C. § 2461(c).

37. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I declare under the penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Eric Field
Special Agent
United States Federal Bureau of Investigation

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 this 15th day of September, 2023.

HONORABLE SHIRLEY P. MENSAH
United States Magistrate Judge
Eastern District of Missouri